UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

JAMES W. SCHOTTEL, JR., et al.,	)	
	)	
Plaintiffs,	)	
	)	
vs.	)	Case No. 4:25-CV-122
	)	
CHANGE HEALTHCARE LLC,	)	**CLASS ACTION COMPLAINT**
	)	
Defendant.	)	**JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

COMES NOW Plaintiff James W. Schottel, Jr., et al., individually and on behalf of all others similarly situated (collectively the "Plaintiffs), by and through their attorneys, and for their Class Action Complaint against Defendant Change Healthcare LLC (hereinafter "Defendant Change") and complain and allege upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys and respectfully states to this Honorable Court the following:

I. NATURE OF THE ACTION

Background Facts

1. This is a civil class action brought individually by Plaintiffs on behalf of recipients of Defendant Change's services.

2. Plaintiff James W. Schottel, Jr. is an individual residing in St. Louis, Missouri in this Eastern District of Missouri

3. Defendant Change is a Limited Liability Company formed in the State of Delaware, with its principal place of business in Nashville, Tennessee.

4. Defendant Change works with many doctors, health insurance plans, and other health companies to help provide health services or benefits that involve Plaintiffs' personal data, including Plaintiffs' name, address, date of birth, phone number, email address, Social Security number, driver's license or state ID number, or other ID number, health insurance data (such as health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers), health data (such as medical record numbers, doctors, diagnoses, medicines, test results, images, care, and treatment), and billing, insurance claims and payment data (such as claim numbers, account numbers, billing codes, payment cards, financial and banking, and balance).

Data Breach of Plaintiffs' Personal Information

5. On February 21, 2024, Defendant Change found activity in their computer system. (*See* Plaintiff's Exhibit 1 *attached hereto*).

6. Defendant Change called law enforcement and turned off their systems. *Id*.

7. On March 7, 2024, Defendant Change learned that a cybercriminal was able to see and take copies of data in their computer system; This happened between February 17, 2024 and February 20, 2024. *Id*.

8. Starting on June 20, 2024, Defendant Change began notifying their business customers about what data may have been seen and taken. *Id*.

II. PARTIES

9. Plaintiff James W. Schottel, Jr. is a resident and citizen of the County of St. Louis, Missouri.

10. Other Plaintiffs injured are residents and citizens of this State of Missouri.

11. Defendant Change Healthcare LLC is a limited liability company with its principal place of business at 424 Church St., Suite 1400, Nashville, TN 37219.

III. JURISDICTION AND VENUE

12. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a)(2), because this is a class action filed under Rule 23 of the Federal Rules of Civil Procedure; there are likely at least hundreds of thousands Class members.

13. The amount in controversy in this class action exceeds $75,000.00, exclusive of interest and costs and there are numerous Class members who are citizens of this state of Missouri other than the Defendant's state of citizenship of Tennessee.

14. This Court also has subject-matter jurisdiction over Plaintiff's and Class members' claims pursuant to 28 U.S.C. § 1367(a).

15. This Court has personal jurisdiction over Defendant Change in this matter because the acts and omissions giving rise to this action occurred in the State of Missouri.

16. This Court has personal jurisdiction over Defendant PSC in this matter because the acts and omissions giving rise to this action occurred in the State of Missouri.

17. Venue is proper in this Eastern District of Missouri pursuant to 28 U.S.C. § 1391(b)(2) and (c) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this Eastern District of Missouri and because the Defendant transacts business and/or has agents within this Eastern District of Missouri and has intentionally availed itself to the laws and markets within this Eastern District of Missouri.

IV. FACTS

18. Class members received a letter dated September 3, 2024 from Defendant Change informing the following:

(a) Defendant Change found activity in their computer system;

(b) Defendant Change called law enforcement and turned off their systems;

(c) On March 7, 2024, Defendant Change learned that a cybercriminal was able to see and take copies of data in their computer system; This happened between February 17, 2024 and February 20, 2024; and

(d) Starting on June 20, 2024, Defendant Change began notifying their business customers about what data may have been seen and taken. *Id*.

19. Plaintiff asserts claims for himself and on behalf of a statewide Class Members for Defendant Change's negligence, negligence per se, and unjust enrichment, for themself and on behalf of the Class, for Defendant's violation of privacy laws.

20. Plaintiff seeks monetary damages, declaratory and injunctive relief, and other remedies for violations of federal and state statutes and the common law.

A. Defendant Change Had Notice of Data Breaches, Particularly Involving the Vulnerability of Such Cyberattacks.

21. Defendant was well aware that their computer system was vulnerable to data breaches.

22. Defendant was also well aware of the likelihood and repercussions of cyber security threats, including data breaches, having observed numerous other well-publicized data breaches involving major corporations over the last few years alone—including Equifax and Facebook—as well as the numerous other similar data breaches preceding those blockbuster breaches.

23. In September 2015, credit reporting agency Experian acknowledged that an unauthorized party accessed one of its servers containing the names, addresses, dates of birth, driver's license, and additional Personal Information of more than 15 million consumers over a period of two years.

B. Defendant Change Failed to Comply with Industry Standards.

24. Following the Equifax data breach, Senator Elizabeth Warren commissioned an investigation and, in February 2018, Senator Warren's office released the results of the 5-month investigation, setting forth a number of findings regarding Equifax's data breach, including the inadequate data security practices that contributed to the data breach (hereinafter the "Warren Report").[1]

25. Senator Warren's investigation revealed that the Equifax data breach was made possible because Equifax adopted weak cyber security measures that failed to protect consumer data and information falling within the Personal Information at issue in this Class Action. (Warren Report, at 3).

26. Senator Warren consulted with industry experts, and the Warren Report concluded that companies that hold large amounts of sensitive data—including Personal Information at issue here—should have multiple layers of cyber security, including: (a) frequently updated tools to prevent hackers from breaching their systems; (b) controls that limit hackers' ability to move throughout their systems in the event of an initial breach; (c) restrictions on hackers' ability to access sensitive data in the event of an initial breach; and (d) procedures to monitor and log all unauthorized access in order to stop the intrusion as quickly as possible. *Id.*

27. Much like the Defendant here, Senator Warren warned that "Despite collecting data on hundreds of millions of Americans without their permission, Equifax failed to fully and effectively adopt any of these four security measures." *Id.*

[1] The Office of Senator Elizabeth Warren, *Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information*, (February 2018), https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf (last visited Sep. 20, 2024).

28. Despite these well-publicized data breaches, a Senate report and other expert reports, Defendant failed to heed the recommendations and inexplicably left sensitive files—and the Personal Information which rested thereon—in a vulnerable manner and available to even the most basic cyber-attack.

C. Defendant Change Data Breach Caused Harm and Will Result in Additional Fraud.

29. Without detailed disclosure to the nearly hundreds of thousands, or more, affected people, including Plaintiff and the Class members, these people have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of their Personal Information without being able to take necessary precautions to prevent imminent harm.

30. Plaintiff has and will incur costs associated with purchasing credit monitoring services.

31. The ramifications of Defendant's failures to keep Plaintiff's and the Class members' Personal Information secure are severe.

32. The Federal Trade Commission (hereinafter the "FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2]

33. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." Id.

34. Identity thieves can use Personal Information, such as that of Plaintiff's and the other Class members', which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims; For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but

[2] 17 C.F.R § 248.201 (2013).

with another's picture; using the victim's Personal Information to obtain government benefits; or filing a fraudulent tax return using the victim's Personal Information to obtain a fraudulent refund.

35. According to the Identity Theft Resource Center® (ITRC), a nationally recognized nonprofit organization established to support victims of identity crime; in 2023, the ITRC tracked 3,205 data compromises in 2023, 1,404 more than in 2022; an increase of 78%.[3]

36. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used; According to the U.S. Government Accountability Office ("GAO"), which previously conducted a study regarding data breaches:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

See GAO, *Report to Congressional Requesters*, p. 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 30, 2025).

37. Thus, Plaintiff and the other Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights; The Class are incurring and will continue to incur such damages in addition to any fraudulent opening of credit cards in their name, any charges incurred in their name and the resulting loss of said fraudulent action, whether or not such charges are ultimately reimbursed by the credit card companies.

38. Further, hackers who obtain a person's Personal Information, can send very authentic-looking emails to persons containing links within the mail that, when clicked will infect

[3] Identity Theft Resource Center, *Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High*, (Jan. 25, 2024), https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/ (last visited Jan. 30, 2025).

the person's computer with malware (often referred to as "phishing emails." A person with a computer infected with malware will lose the use of the computer and cost the person several hundred dollars in computer repair.

D. Plaintiff and the other Class Members Suffered Damages

39. Plaintiff's and the other Class members' Personal Information is private and sensitive in nature, and was left inadequately protected, if not completely unprotected, by Defendant; Defendant did not obtain Plaintiff's or the other Class members' consent to disclose their Personal Information to any other person or entity, as required by applicable law and industry standards.

40. The data breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and the other Class members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and the other Class members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

41. Defendant had the resources to prevent a breach; Defendant made significant expenditures to market its products and touted its data security as industry leading, but neglected to adequately invest in data security, despite the growing number of Personal Information exfiltrations, as well as several years of well-publicized data breaches.

42. Had Defendant remedied the deficiencies in its database and computer systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would not have subjected its computer systems containing Plaintiff's and Class

members' Personal Information to cyberattacks, and instead would have prevented the dissemination of Personal Information of approximately hundreds of thousands of persons, or more.

43. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiff's and the other Class members have been placed in an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the data breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, changing the information used to verify their identity to information not subject to this data breach, and potentially filing police reports. This time has been lost forever and cannot be recaptured.

44. The injuries suffered by Plaintiff and the Class as a direct result of the data breach include, but are not limited to:

(a) theft of their Personal Information;

(b) the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including ascertainable costs for purchasing credit monitoring services and identity theft protection services and the stress, nuisance and annoyance of dealing with all such issues resulting from the data breach;

(c) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' Personal Information on the Internet black market;

(d) being subjected to having malware infect their computer from opening an email appearing to be an authentic email prepared and sent by a hacker using the compromised Personal Information, costs in repairing a malware-infected computer and costs in purchasing additional computer malware protection;

(e) the untimely and inadequate notification of the data breach;

(f) the improper disclosure of their personal data;

(g) loss of privacy;

(h) ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

(i) ascertainable losses in the form of deprivation of the value of their Personal Information, for which there is a well-established national and international market; and

(j) the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, purchasing credit monitoring and identity theft protection services and the stress, nuisance and annoyance of dealing with all such issues resulting from the data breach.

45. Although the Personal Information of Plaintiff and the other Class Members has been stolen, Defendant continues to hold Personal Information of approximately hundreds of thousands of people, or more, including Plaintiff's and the other Class members' Personal Information; Particularly, because Defendant has demonstrated an inability to prevent a data breach or stop it from continuing—even after being detected and informed of the impermissible dissemination—Plaintiff and the other Class Members have an undeniable interest in ensuring their Personal Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further disclosure and theft.

V. CLASS ALLEGATIONS

46. Pursuant to Rules 23(b)(1), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, Plaintiff asserts that common law claims against the Defendant for negligence, negligence per se, bailment, and unjust enrichment, declaratory and injunctive relief, and the various consumer protection laws, on behalf of themselves and the following class (the "Class"):

STATEWIDE CLASS:

All residents of the State of Missouri whose Personal Information was compromised as a result of the data breach.

47. Pursuant to Rules 23(a)(1), (a)(2), (a)(3), and (a)(4) of the Federal Rules of Civil Procedure, Plaintiffs assert statutory claims under state data breach statutes.

Numerosity: Rule 23(a)(1) of the Federal Rules of Civil Procedure

48. The members of the Class are so numerous that individual joinder of all Class members is impracticable.

49. Plaintiff is informed and believes—based on the size of the exposed computer systems—that there are approximately 400,000 to 500,000 Class members or more; Those individuals' names and addresses are available from Defendant's records, and Class members may

be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice.

Commonality and Predominance:
Rules 23(a)(2) and 23(b)(3) of the Federal Rules of Civil Procedure

50. This action involves common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

(a) Whether Defendant knew or should have known that its computer system was susceptible to data breaches and the Personal Information stored therein;

(b) Whether Defendant knew or should have known that the files stored in its computer system containing Plaintiff's and Class members' Personal Information kept therein, was properly encrypted or unencrypted;

(c) Whether Defendant failed to take adequate and reasonable measures to ensure files stored in its computer system containing Plaintiff's and Class members' Personal Information were protected;

(d) Whether Defendant failed to take available steps to prevent and stop the data breach from occurring;

(e) Whether Defendant failed to disclose the material facts that they did not have adequate security practices to safeguard Plaintiff's and Class members' Personal Information;

(f) Whether Defendant failed to provide timely and adequate notice of the data breach;

(g) Whether Defendant owed a duty to Plaintiff and other Class members to protect their Personal Information and to provide timely and accurate notice of the data breach to Plaintiff and other Class members;

(h) Whether Defendant breached its duties to protect the Personal Information of Plaintiff and other Class members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiff and other Class members of the data breach;

(i) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer system, resulting in the unauthorized access and/or theft of approximately 400,000 to 500,000, or more, patient's Personal Information;

(j) Whether Defendant's conduct renders them liable for negligence, negligence *per se*, and unjust enrichment;

(k) Whether, as a result of Defendant's conduct, Plaintiff and other Class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

(l) Whether, as a result of Defendant's conduct, Plaintiff and other Class members are entitled to injunctive, equitable, declaratory, and/or other relief, and, if so, the nature of such relief.

Typicality: Rule 23(a)(3) of the Federal Rules of Civil Procedure

51. Plaintiff's claims are typical of the other Class members' claims because Plaintiff and the other Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

Adequacy of Representation: Rule 23(a)(4) of the Federal Rules of Civil Procedure

52. Plaintiff is an adequate class representative because his interests do not conflict with the interests of the other Class members who he seeks to represent, Plaintiff has retained competent counsel and experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

53. The Class' interests will be fairly and adequately protected by Plaintiff.

Declaratory and Injunctive Relief: Rule 23(b)(2) of the Federal Rules of Civil Procedure

54. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendant.

55. Such individual actions would create a risk of adjudications, which would be dispositive of the interests of other Class members and impair their interests.

56. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

Superiority: Rule 23(b)(3) of the Federal Rule of Civil Procedure

57. A class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action.

58. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct.

59. Even if Class members could afford litigation, the court system could not; Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED ON BEHALF OF THE CLASS

COUNT I

NEGLIGENCE
AGAINST CHANGE HEALTHCARE LLC
(Asserted by Plaintiff, individually, and on behalf of the Class)

60. Plaintiffs re-allege all of the preceding paragraphs as if set forth fully herein.

61. Defendant owed a duty to Plaintiff and the other Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, handling, transferring and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

62. This duty included, among other things, designing, maintaining, transferring and testing Defendant's computer system to ensure that Plaintiff's and the other Class members' Personal Information in Defendant's possession was adequately secured and protected.

63. Defendant further owed a duty to Plaintiff and the other Class members to implement processes that would detect a breach of its computer system in a timely manner and to

timely act upon warnings and alerts, including those generated by its own electronic and security systems.

64. Defendant owed a duty to Plaintiff and the other Class members to provide security, including consistent with industry standards and requirements, to ensure that its computer system and computer networks, and the personnel responsible for them, adequately protected the Personal Information of Plaintiff and the other Class members about whom Defendant collected, maintained, and used such information.

65. Defendant owed a duty of care to Plaintiff and the other Class members because, as patients, they were foreseeable and probable victims of any inadequate security practices.

66. Defendant solicited patients' insurance carriers, gathered, and stored the Personal Information provided by Plaintiff and the other Class members to facilitate its products to customers.

67. Defendant knew it inadequately maintained its computer system files containing Personal Information of Plaintiff and the other Class members and knew or should have known that such information was susceptible to a data breach and not subject to any reasonable data security measures.

68. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Defendant.

69. Various FTC publications and data security breach orders further form the basis of Defendant's duty; additionally, individual states have enacted statutes based upon the FTC Act that also create a duty.

70. Defendant knew that a breach of its computer system would cause damages to Plaintiff and the other Class members and Defendant had a duty to adequately protect such sensitive Personal Information.

71. Defendant owed a duty to timely and accurately disclose to Plaintiff and the other Class members that their Personal Information had been or was reasonably believed to have been compromised.

72. Timely disclosure was required, appropriate, and necessary so that, among other things, Plaintiff and the other Class members could take appropriate measures to change the information used to verify their identity to information not subject to this data breach, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

73. Defendant knew, or should have known, of the risks inherent in collecting, storing and transferring the Personal Information of Plaintiff and the other Class members and of the critical importance of providing adequate security of that information.

74. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and the other Class and Subclass members; Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the data breach as set forth herein and also includes their decisions not to comply with industry standards for the safekeeping and maintenance of the Personal Information of Plaintiffs and the other Class and Subclass members.

75. Defendant breached the duties it owed to Plaintiff and the other Class members by failing to exercise reasonable care and implementing adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiff and the other Class members.

76. Defendant breached the duties it owed to Plaintiff and the other Class members by failing to properly implement technical systems or security practices that could have prevented the dissemination and loss of the Personal Information at issue.

77. Defendant breached the duties it owed to Plaintiff and the other Class members by failing to properly maintain their sensitive Personal Information; Given the risk involved and the amount of data at issue, Defendant's breach of its duties was entirely unreasonable.

78. Defendant breached its duties to timely and accurately disclose that Plaintiff's and the other Class members' Personal Information in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

79. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the other Class members, their Personal Information would not have been compromised.

80. The injuries and harm suffered by Plaintiff and the other Class members, as set forth above, was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Personal Information within Defendant's possession; Defendant knew or should have known that its computer system and technologies for processing, securing, safeguarding, transferring electronic files and deleting Plaintiff's and the other Class members' Personal Information were inadequate and vulnerable to being breached by hackers.

81. Plaintiff and the other Class members suffered injuries and losses described herein as a direct and proximate result of Defendant's conduct resulting in the data breach, including

Defendant's lack of adequate reasonable and industry standard security measures; Had Defendant implemented such adequate and reasonable security measures, Plaintiff and the other Class members would not have suffered the injuries alleged, as the data breach would likely have not occurred.

82. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the other Class members have suffered injury and the significant risk of harm in the future and are entitled to damages in an amount to be proven at trial.

WHEREFORE, for the foregoing reasons, Plaintiffs pray for judgment in their favor and against Defendant Change Healthcare LLC, and damages for any and all loses or damages they have suffered; punitive damages against Defendant Change Healthcare LLC in such sum, according to proof, that will serve to punish it and to deter it and others from like conduct; costs of this action; and for such other and further relief that is just and proper under the circumstances.

COUNT II

NEGLIGENCE PER SE
AGAINST CHANGE HEALTHCARE LLC
(Asserted by Plaintiff, individually, and on behalf of the Class)

83. Plaintiff re-alleges all of the preceding paragraphs as if set forth fully herein.

84. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies—such as Defendant—of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Defendant's duty.

85. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry

standards; Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach.

86. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

87. The Class is within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect, as the Defendant is engaged in trade and commerce and Defendant bears primary responsibility for reimbursing consumers for fraud losses; Plaintiff and absent class members are consumers.

88. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against; Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

89. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and the other Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including, but not limited to:

(a) theft of their Personal Information;

(b) the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including ascertainable costs for purchasing credit monitoring services and identity theft protection services and the stress,

nuisance and annoyance of dealing with all such issues resulting from the data breach;

(c) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' Personal Information on the Internet black market;

(d) being subjected to having malware infect their computer from opening an email appearing to be an authentic email prepared and sent by a hacker using the compromised Personal Information, costs in repairing a malware-infected computer and costs in purchasing additional computer malware protection;

(e) the untimely and inadequate notification of the data breach;

(f) the improper disclosure of their personal data;

(g) loss of privacy;

(h) ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

(i) ascertainable losses in the form of deprivation of the value of their Personal Information, for which there is a well-established national and international market; and

(j) the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, purchasing credit monitoring and identity theft protection

services and the stress, nuisance and annoyance of dealing with all such issues resulting from the data breach.

90. Although the Personal Information of Plaintiff and the other Class members has been stolen, Defendant continues to hold Personal Information of over millions people, including Plaintiff's and the other Class members' Personal Information.

91. Particularly, because Defendant has demonstrated an inability to prevent a data breach or stop it from continuing—even after being detected and informed of the impermissible dissemination—Plaintiff and the other Class members have an undeniable interest in ensuring their Personal Information is secure, remains secure, is properly and promptly destroyed when appropriate and is not subject to further disclosure and theft.

WHEREFORE, for the foregoing reasons, Plaintiffs pray for judgment in their favor and against Defendant Change Healthcare LLC, and damages for any and all loses or damages they have suffered; punitive damages against Defendant Change Healthcare LLC in such sum, according to proof, that will serve to punish it and to deter it and others from like conduct; costs of this action; and for such other and further relief that is just and proper under the circumstances.

COUNT III

UNJUST ENRICHMENT
AGAINST CHANGE HEALTHCARE LLC
(Asserted by Plaintiff, individually, and on behalf of the Class)

92. Plaintiff re-alleges all of the preceding paragraphs as if set forth fully herein.

93. Defendant collected, maintained, and permitted Plaintiff's and the other Class members' and others' Personal Information to be obtained by other persons without the knowledge or direct consent of Plaintiff, the other Class members and others.

94. Defendant appreciates or has knowledge of the benefits conferred directly upon them by Plaintiff, the other Class members and others.

95. As a result of Defendant's wrongful conduct, as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff, the other Class members and others.

96. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and the other Class members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

97. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff, the other Class members and others, in an unfair and unconscionable manner.

98. Defendant's retention of such benefits under the circumstances making it inequitable to do so and constitutes unjust enrichment.

99. Plaintiff, the other Class members and others did not confer these benefits officiously or gratuitously and it would be inequitable and unjust for Defendant to retain these wrongfully obtained profits.

WHEREFORE, for the foregoing reasons, Plaintiffs pray for judgment in their favor and against Defendant Change Healthcare LLC, and damages for any and all loses or damages they have suffered; punitive damages against Defendant Change Healthcare LLC in such sum, according to proof, that will serve to punish it and to deter it and others from like conduct; costs of this action; and for such other and further relief that is just and proper under the circumstances.

COUNT IV

DECLARATORY AND INJUNCTIVE RELIEF AGAINST CHANGE HEALTHCARE LLC
(Asserted by Plaintiff, individually, and on behalf of the Class)

100. Plaintiff re-alleges all of the preceding paragraphs as if set forth fully herein.

101. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 et seq., this Honorable Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief; Furthermore, this Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this Complaint.

102. An actual controversy has arisen in the wake of the data breach regarding Defendant's common law, statutory, and other duties to reasonably safeguard Plaintiff's, the other Class members' and others' Personal Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff, the other Class members and others from further data breaches that compromise their Personal Information.

103. Plaintiff alleges that Defendant's data security measures were and remain inadequate.

104. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Personal Information and remain at imminent risk that further compromises of his Personal Information will occur in the future.

105. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Defendant owed and continues to owe a legal duty to secure Plaintiff's, the other Class members' and others' Personal Information and to timely notify

consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

(b) Defendant continues to breach its legal duties by failing to employ reasonable measures to secure Plaintiff's, the other Class members' and others' Personal Information.

106. This Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect Plaintiff's, the other Class members' and others' Personal Information.

107. If an injunction is not issued, Plaintiff will suffer additional irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant's handling electronic files containing Plaintiff's, the other Class members' and others' Personal Information.

108. The risk of another such data breach is real, immediate, and substantial.

109. The hardship to Plaintiff, if an injunction does not issue, exceeds the hardship to Defendant if an injunction is issued; Among other things, if another massive data breach occurs with Defendant Change Healthcare LLC, Plaintiff will likely be subjected to substantial identify theft and other damage; On the other hand, the cost to Defendant of complying with an injunction by employing reasonable data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

110. Issuance of the requested injunction will not disserve the public interest; To the contrary, such an injunction would benefit the public by preventing another data breach of Defendant's computer system, thus eliminating the additional injuries that would result to Plaintiff, the other Statewide Class members and others whose Personal Information would be further compromised.

REQUEST FOR RELIEF

WHEREFORE, for the foregoing reasons, Plaintiff, individually and on behalf of the Class members, respectfully request this Honorable Court to enter judgment in their favor and against Defendant on Count IV, and as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiff as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiff and the other Class Members actual, direct (where actual and direct damages are separate under the law), compensatory, consequential, and general damages in an amount to be determined at trial;

4. Declare that Change Healthcare LLC is financially responsible for notifying all Class members of the data breach and the release of the Class members' Personal Information;

5. That the Court Order that Defendant shall audit, for the past five (5) years and reassess all prior electronic files of their computer system of medical patients;

6. That the Court Order disgorgement and restitution of all earnings, profits, compensation, and benefits Defendant have received as a result of its unlawful acts, omissions, and practices;

7. That the Court award statutory damages, and punitive or exemplary damages, to the extent permitted by law;

8. That the unlawful acts alleged in this Complaint be adjudged and decreed to be negligent, negligent per se, and unjust enrichment;

9. That Plaintiff be granted the declaratory relief sought herein;

10. That the Court award to Plaintiff reasonable attorneys' fees, including expert witness fees, and award to Plaintiff fees and expenses in the prosecution of this action;

11. That the Court award pre-judgment and post-judgment interest at the maximum legal rate allowed by law; and

12. That the Court grant all such other relief as it deems just and proper under the circumstances.

DATED: January 30, 2025.

Respectfully submitted,

SCHOTTEL & ASSOCIATES, P.C.

BY: s/*James W. Schottel, Jr.*

James W. Schottel, Jr. #51285MO
906 Olive St., PH
St. Louis, MO 63101
(314) 421-0350
(314) 421-4060 facsimile
jwsj@schotteljustice.com

Pro se Plaintiff
James W. Schottel, Jr.